Sean Hoar, Partner & Chair
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
shoar@constangy.com
Telephone: 503.376.5932

June 13, 2026

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

Re: Notification of Data Security Incident

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP represents Surplus Line Association of California ("SLA of California"), located at 12667 Alcosta Boulevard, Ste 450, San Ramon, CA 94583, in connection with its response to a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the of the impact to Nebraska residents in accordance with Nebraska's data breach notification statute.

1. Nature of the Security Incident

On or around April 14, 2026, SLA of California became aware of suspicious activity within its network environment and promptly initiated an investigation. In response, SLA of California engaged independent cybersecurity specialists to assist with the process. As a result of the investigation, it was determined that certain files were accessed and acquired without authorization on April 4, 2026. SLA of California engaged a third-party vendor to perform a comprehensive review of those files and, on June 15, 2026, learned that certain personal information was contained within the potentially affected data. SLA of California then took steps to notify the affected individuals as soon as possible.

2. Number of Affected Nebraska Residents & Information Involved

The incident involved personal information for approximately 8 Nebraska residents. The information involved in the incident for the affected Nebraska residents included name and Social Security number.

3. Notification to Affected Individuals

On June 13, 2026, a notification letter was sent to the affected residents by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The notification letter also offers individuals the opportunity to enroll in 12 months of complimentary identity protection services through TransUnion, including credit monitoring and a $1,000,000 identity theft insurance policy. A sample notification letter sent to the impacted individuals is included with this correspondence.

4. Measures Taken to Address the Incident

As referenced above, upon discovering this incident, SLA of California took immediate steps to investigate. SLA of California also reported the incident to the FBI and the California Department of Insurance and will continue to assist them in their investigation. Finally, SLA of California is in the process of notifying the potentially affected individuals and providing them with steps they can take to protect their personal information and offering the remediation services referenced above. SLA of California has also established a toll-free call center through TransUnion to answer questions about the incident and address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at shoar@constangy.com or 503.459.7707 or Madison Balasek at mbalasek@constangy.com or 415.918.3007.

Sincerely,

Sean B. Hoar

Sean B. Hoar
Partner & Chair, Cybersecurity & Data Privacy Team

Encl.: Sample Notification Letter

Surplus Line Association of California
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS4252

0001053

5_0001053

[redacted]

July 13, 2026

Subject: Notice of Data Security Incident

Dear [redacted]:

Surplus Line Association of California ("SLA of California") is writing to inform you of a recent data security incident that may have affected your personal information. SLA of California takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On or around April 14, 2026, SLA of California became aware of suspicious activity within its network environment and promptly initiated an investigation. SLA of California also engaged independent cybersecurity specialists to assist with the process. The investigation determined that certain files were accessed and acquired without authorization on April 4, 2026. SLA of California engaged a third-party vendor to perform a comprehensive review of those files and, on June 15, 2026, learned that some of your personal information was contained within the potentially affected data. SLA of California then took steps to notify you as soon as possible.

What Information Was Involved. The information may have included your first and last name and Social Security number.

What We Are Doing. As soon as SLA of California discovered this incident, it took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. SLA of California also notified the California Department of Insurance and the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold perpetrators accountable. SLA of California is also offering you complimentary identity theft protection services, including credit monitoring and a $1,000,000 identity theft insurance policy. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. These services are provided through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in the complementary credit monitoring and identity theft protection services, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered with TransUnion by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-844-593-5372 Monday through Friday from 5:00 am to 5:00 pm PST, excluding major U.S. holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Surplus Line Association of California

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.